سیستم مرکزی

مدیریت کلمه عبور

پائیز ۱۴۰۳

رضا حجی زاده

طرح مسئله

با توجه رشد روز افزون سامانه ها و سیستم های کاربردی مسئله ی نگهداری از دسترسی ها[1] را به یکی از چالشهای امروز هر کاربر تبدیل کرده است. حق دسترسی یا به اصطلاح همان ترکیب نام کاربری/کلمه عبور[2] است که سامانه نرم افزاری بر اساس آن می تواند علاوه بر احراز هویت[3]، سطح دسترسی[4] کاربر را هم تعیین کند. امروزه کاربران در حوزه ی نگهداری از نام کاربری/کلمه عبور با دو مسئله روبرو هستند:

۱- تعداد زیاد نام کاربری/کلمه عبور به دلیل گسترش روزافزون سامانه های مجازی
۲- نگهداری امن اطلاعات نام کاربری/کلمه عبور با توجه به گسترش روزافزون حملات سرقت و جعل اطلاعات هویتی

علاوه بر موارد فوق که هر کاربر حقیقی با آنها مواجه است موضوع اشتراک گذاری نام کاربری/کلمه عبور بین پرسنل سازمان/شرکت موردی است که فقط اشخاص حقوقی با آن مواجه هستند. با توجه به اینکه سازمانها و شرکت ها برای دریافت خدمات از شرکای[5] خود بعنوان یک شخصیت حقوقی شناخته شده و فقط یک نام کاربری/کلمه عبور واحد دارند باید تدابیری اتخاذ کنند که به نحوی این حق دسترسی را بین کارشناسان خود که با این خدمت مرتبط هستند اشتراک گذاری کنند.

به دلیل افزایش سرویس های مجازی شرکای تجاری سازمان ها و شرکت ها و به تبع آن تعدد نام کاربری/کلمه عبور که باید در اختیار کارکنان قرار گیرد عملا استفاده از روشهای سنتی مانند اشتراک گذاری از طریق ایمیل، چت سازمانی، پیامک و... کارآمد نبوده و باید به دنبال یک روش نگهداری و اشتراک گذاری متمرکز باشیم که قرار است در این مقاله به بررسی روشهای موجود و انتخاب یکی از این روشها بپردازیم.

دو مقوله ی نگهداری و اشتراک گذاری نام کاربری/کلمه عبور را می توان از چند جنبه ی مختلف مورد بررسی قرار داد:

خطرات امنیتی: بدون یک راه حل متمرکز مدیریت رمز عبور، کارمندان اغلب به اقدامات ناامن مانند استفاده از رمزهای عبور ضعیف، استفاده مجدد از کلمه عبور در چندین سرویس یا اشتراک گذاری رمز عبور از طریق کانال های ناامن

---

[1] Credentials
[2] Username / Password
[3] Authentication
[4] Authorization
[5] Stakeholders

مانند ایمیل یا برنامه های پیام رسانی متوسل می شوند. این اقدامات به طور قابل توجهی خطر نقض امنیت و به خطر افتادن داده ها را افزایش می دهد.

ناکارآمدی عملیاتی: تیم ها زمان قابل توجهی را برای مدیریت، اشتراک گذاری و بازیابی رمزهای عبور تلف می کنند. زمانی که اعضای تیم نیاز به دسترسی به حساب‌های مشترک دارند یا زمانی که کارکنان سازمان را ترک می‌کنند، مدیریت دستی[۶] رمز عبور عملی زمان‌بر و مستعد خطا می‌شود. این ناکارآمدی روی بهره وری تأثیر منفی دارد.

نگرانی های مربوط به نهادهای نظارتی: سازمان ها باید از مقررات و استانداردهای امنیتی مختلف حفاظت از داده ها[۷] پیروی کنند. بدون سیستم های مناسب مدیریت رمز عبور، اجرای سیاست های دسترسی و نشان دادن انطباق با دستورالعمل استانداردها بسیار دشوار می شود و به طور بالقوه سازمان را در معرض مخاطرات حقوقی از سمت سازمانهای نظارتی قرار می دهد.

پیچیدگی کنترل دسترسی[۸]: با رشد، سازماندهی مجدد تیم ها یا تغییر نقش کارکنان در سازمان، مدیریت اینکه چه کسی به کدام سیستم دسترسی داشته باشد پیچیده تر می شود. شرکت‌ها به روشی دقیق برای کنترل اشتراک‌گذاری رمز عبور نیاز دارند تا اطمینان حاصل کنند که اعضای تیم فقط به منابع لازم برای نقش‌هایشان دسترسی دارند و در عین حال امکان تغییر سریع یا لغو دسترسی در صورت نیاز نیز وجود داشته باشد.

این چالش‌ها بر نیاز حیاتی به یک راه‌حل مدیریت رمز عبور سازمانی[۹] تاکید می کند که مکانیزم های ذخیره‌سازی امن کلمات عبور، احراز هویت، اشتراک‌گذاری کنترل‌شده و ثبت گزارش[۱۰] دسترسی به کلمات عبور را پیاده سازی کرده باشد.

---

[6] Manual

[۷] مانند GDPR

[8] Access control

[9] Enterprise Password Management Solution

[10] Log

شرح وضعیت فعلی

در حال حاضر برای اشتراک گذاری کلمات عبور بین اعضای تیم ها مکانیزم مشخصی وجود ندارد و معمولا کلمات عبور از طریق گوگل شیت یا در چت سازمانی یا حتی شبکه های اجتماعی بین اعضا اشتراک گذاری می شود که این روش می تواند مخاطرات امنیتی زیادی به همراه داشته باشد.

از مهمترین مشکلات فعلی این روش می توان به این موارد اشاره کرد:

- نگهداری کلمات عبور بصورت فاش و بدون استفاده از هیچ مکانیزم رمزنگاری
- عدم امکان مدیریت دسترسی به کلمات عبور بر اساس شرح وظیفه
- عدم امکان گزارش گیری بر اساس نقش
- عدم تغییر رمزهای عبور بعد از خروج عضو از تیم
- عدم وجود مکانیزم احراز هویت برای دسترسی به کلمات عبور
- عدم امکان مکانیزمی برای جلوگیری از کپی، توزیع و انتشار فایل کلمات عبور

راه حل های موجود

با توجه به بررسی و نیازسنجی انجام شده به نظر می رسد ابزار مورد استفاده برای مدیریت کلمه عبور در شرکت باید نیازمندی های زیر را داشته باشد:

۱- به دلیل محدودیت های مالی، حتی المقدور از ابزارهای بدون لایسنس تجاری استفاده شود.
۲- به جهت شفافیت در الگوریتم های رمزنگاری، احراز هویت، ذخیره سازی و... از ابزارهای متن باز استفاده شود
۳- به جهت سهولت در دسترسی به کلمات عبور برنامه[11] ای برای سیستم عامل های مختلف داشته باشد
۴- امکان پیاده سازی سرویس در سازمان[12] وجود داشته باشد و نیازی به استفاده از ابزارهای ابری عمومی نباشد.
۵- امکان تامین امنیت در هر دو سطح ذخیره سازی[13] و انتقال[14] داده وجود داشته باشد
۶- حتی المقدور افزونه هایی برای مرورگرهای مختلف داشته باشد
۷- به جهت امکان دسترسی از هر نقطه امکان دسترسی از طریق وب[15] نیز وجود داشته باشد
۸- امکان دسترسی به کلمات عبور بر اساس نقش کاربران[16] وجود داشته باشد
۹- امکان گزارش گیری[17] از دسترسی ها وجود داشته باشد
۱۰- امکان غیرفعال کردن دانلود یکجای[18] کلمات عبور
۱۱- امکان احراز هویت کاربران با ابزارهای LDAP شناخته شده مانند اکتیو دایرکتوری وجود داشته باشد.
۱۲- امکان پیاده سازی مکانیزم های چندعملی احراز هویت[19] وجود داشته باشد.
۱۳- امکان پشتیبان گیری و بازیابی کلمات عبور وجود داشته باشد.
۱۴- امکان برقراری ارتباط با رابط API به جهت خودکارسازی برخی فعالیتها

از مجموع قابلیت های فوق فقط موارد ۳ و ۶ بعنوان قابلیت های ارزش افزوده هستند و مابقی موارد بعنوان موارد لازم و ضروری ابزار مورد استفاده هستند.

---

[11] Application
[12] On-premises
[13] Data in rest
[14] Data in transit
[15] Web-based
[16] Role-based access control
[17] Audit logging and reporting
[18] Disable password export
[19] Multi-factor authentication

ابزارهای زیادی بعنوان سامانه مدیریت کلمات عبور وجود دارد که از مهمترین آنها می توان به موارد زیر اشاره کرد:

۱۵- Bitwarden Enterprise
۱۶- KeyPass Enterprise
۱۷- ManageEngine password Manager Pro
۱۸- 1Password Business
۱۹- Passbolt
۲۰- HashiCorp Vault

در جدول شماره ۱ مقایسه ای بین این ابزارها بر اساس قابلیت های مورد نیاز سازمان ارائه شده است.

بر اساس جدول شماره ۱ و بر اساس نیازهای ضروری، ابزارهای Keypass, ManageEngine, 1Password به دلیل متن باز نبودن از گردونه رقابت حذف می شوند.

ابزار Hashicorp فقط برای نگهداری کلمه عبور[۲۰] نیست و از آن می توان برای نگهداری سایر داده های محرمانه[۲۱] نیز استفاده کرد. این ابزار می تواند برای مدیریت زیرساخت/DevOps/مرکز داده نیز مورد استفاده قرار گیرد.

پیاده سازی Bitwarden از دو ابزار دیگر راحت تر بوده، جامعه توسعه دهندگان بیشتری دارد و برای مدیریت کلمه عبور در سازمانهای کوچک مناسب تر است.

[20] Password
[21] Secret

Feature	Bitwarden Enterprise	KeyPass Enterprise	ManageEngine Password Pro	1Password Business	Passbolt	HashiCorp Vault
Primary Features						
Purchase License	Yes (also free)	Yes	Yes	Yes	Yes	Yes (also free)
Open Source	Yes (AGPL-3.0)	No	No	No	Yes (AGPL-3.0)	Yes (MPL 2.0)
Multi-OS Support	All major OS	Windows-focused	All major OS	All major OS	All major OS	All major OS
On-premise Deployment	Yes	Yes	Yes	No	Yes	Yes
Data at Rest Security	AES-256	AES-256	AES-256	AES-256	GPG	AES-256/GCM
Data in Transit Security	TLS 1.2/1.3	TLS 1.2	TLS 1.2	TLS 1.2/1.3	TLS 1.2	TLS 1.2/1.3
Browser Add-ons	All major browsers		major browsers	All major browsers	Firefox/Chrome	No official
Web-based Access	Yes	Yes	Yes	Yes	Yes	Yes
Role-based Access	Yes	Yes	Yes	Yes	Yes	Yes
Reporting and Logging	Comprehensive	Basic	Advanced	Comprehensive	Advanced	Advanced
Export Disable	Yes	Yes	Yes	Yes	Yes	Yes
LDAP/AD Integration	Yes	Yes	Yes	Yes	Yes	Yes
Additional Features						
API Access	Yes	Limited	Yes	Yes	Yes	Yes
Password Generator	Yes	Yes	Yes	Yes	Yes	Yes
Password Strength Analysis	Yes	Basic	Advanced	Yes	Yes	No
Mobile Apps	Yes	Third-party	Yes	Yes	No	No
Emergency Access	Yes	No	Yes	Yes	No	No
Multi-Factor Auth	Multiple options	Basic	Multiple options	Multiple options	Yes	Multiple options
Password History	Yes	Yes	Yes	Yes	Yes	Yes
Secure File Storage	Yes	No	Yes	Yes	No	Yes (binary)
Password Sharing	User/Group based	Basic	Advanced	Vault based	Group based	Policy based
Automated Password Rotation	No	No	Yes	No	No	Yes
Session Management	Yes	Basic	Advanced	Yes	Yes	Advanced
Secret Types Support	Passwords only	Passwords only	Multiple types	Multiple types	Passwords	All types
Custom Fields	Yes	Yes	Yes	Yes	Yes	Yes
Backup/Recovery	Yes	Manual	Advanced	Cloud-based	Yes	Backend dependent
SSH Key Management	Basic	No	Yes	Yes	Yes	Advanced
Version Control	Basic	No	Yes	Yes	Yes	Yes

جدول شماره ۱ - مقایسه بین ابزارهای مدیریت کلمه عبور

نتیجه گیری

بر اساس جدول شماره ۱ و توضیحات مرتبط با آن به نظر می رسد در حال حاضر استفاده از ابزار Bitwarden به دلیل ساده تر بودن پیاده سازی، بزرگتر بودن جامعه توسعه دهندگان و بروزرسانی های منظم تر نسبت به رقبای خود گزینه مناسب تری برای شرایط فعلی سازمان می باشد ولی به دلیل نیاز به اشتراک گذاری کلمات عبور که یکی از نیازمندی‌های مهم سازمان بوده و این قابلیت در نرم افزار Bitwarden نیازمند پرداخت هزینه است، قابل استفاده نیست. در نتیجه استفاده از این ابزار متناسب با نیازمندی ها و شرایط سازمان نیست و تنها گزینه قابل استفاده Hashicorp Vault است که یک ابزار قدرتمند بوده و علاوه بر اینکه ابزاری برای مدیریت کلمات عبور است قابلیتهای زیاد دیگری از جمله منبع ذخیره سازی توکن های API و کلیدهای SSH نیز می باشد.

جزئیات پیاده‌سازی

با توجه به اینکه امکان نصب و راه اندازی ابزار مدیریت کلمات عبور Hashicorp Vault بصورت کانتینر داکر وجود دارد، بنابراین به سخت افزار خاصی نیاز ندارد و یک ماشین مجازی با حدود 4GB حافظه و ۴ هسته پردازنده و ۳۰ گیگابایت هارد دیسک می تواند این سرویس را به راحتی پردازش کند.

به جهت جلوگیری از قطع درختان سبز از چاپ این مطلب جز در موارد خیلی ضروری خودداری کنید.